Published and Copyright (c) 1999 - 2011
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1344 11/04/11

~ China Scorns at Charges! ~ People Are Talking! ~ CIA Tracks Revolts!
~ US Blasts China, Russia! ~ The Right to Dual-Boot ~ Facebook-Google War!
~ Anonymous Exposes Users! ~ Stupid Hacker Tricks! ~ Copyright and Wrong!

~ Spike TV Gets Award Show ~ ~ New Call of Duty!

-* UK's Cyberattacks Warnings! *-
-* UK Says Internet Power Grab Will Fail *-
-* Video Games Stimulate Kids' Imaginations! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Well, remember last week I mentioned that we were about to get hit by a Nor'easter that weekend? Well, we got hit and hit hard! While we didn't get a large amount of snow in my immediate area, other areas weren't as fortunate - up to 3 feet in areas! And to make matters much worse, the snow was that extremely wet and heavy stuff - not the fluffy light stuff that is easily moved!

The problem with this kind of snow, at this time of the year when leaves are still in abundance on trees, is that the leaves acts as a blanket of sorts and the snow weighs heavily down on them. There were alerts all over the place that warned the citizenry that the chances of downed branches and trees was very high. Well, we could hear the sounds of branches cracking all night. At about 11:15 p.m. on Saturday night, I heard one particular cracking noise that was very close. I looked out various windows to see if it was one of my trees. The pines were okay. The huge oak in the side yard was fine. The oaks near our property in my neighbor's yard were fine. I finally looked out a back window and saw a branch - a large one - overhanging my neighbor's deck. He has no trees, so I knew it was mine. But, it was dark so I couldn't see too clearly. I heard my neighbor's commotion, so I hollered out to make sure everyone was okay; I didn't know how much of the tree (or branch) fell, or if it caused any damage. They responded and said they were okay, so I went to bed because I had to be at work early in the morning.

When I woke up, I looked out my window in my upstairs study to get a better look, The branch was actually a good portion of my tree! In fact, it looked like the tree had split in half, and fallen on my neighbor's garage, deck, and house! I couldn't see any obvious damage from my vantage point, so I let my wife know what I saw, and for her to call my neighbor.

When I got home from work - out early because our store was without power, as was most of the town, I went next door to survey the damage. I spent the rest of the day trying to contact our insurance company, as well as a tree removal service to cut up and remove the tree. It was precariously draped over their garage and up against the sliding door on their deck.

The tree was removed Wednesday, and I saw my insurance agent Thursday. Fortunately, there was little damage to my neighbor's house, etc. So that meant no cost him. My insurance, hopefully, will reimburse me to cut up and remove the tree, and no noteworthy damage on my property. In fact, in talking to my claims adjuster, he told me that taking my

claim report was one of the easiest ones he's taken due to this storm! So, I consider myself and my neighbor to be very fortunate! People are still without power, almost a week after this storm. There has been widespread damage throughout the state, and lives lost due to storm-related issues. It's been a horrific week for many, many people. And the problem is, there's very little one can do to prepare for this type of a storm so early in the Fall season. And we had less than three inches of snow!

Anyway, things are quieting down now and starting to get back to normal. The Halloween celebrations were postponed until tonight, but we decided to forego being a part of this year; we didn't even buy any candy for the little ghosts and goblins who would normally be out canvassing the neighborhood.

So, as we try to finally get some rest from all of the events of the past week, I hope that everyone enjoyed your Halloween festivities - either on Halloween night, or a postponed one. And don't forget, that if you're affected by Daylight Savings Time, set your clocks back an hours this weekend and enjoy and extra hour of sleep!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Video Games Stimulate Kids Imaginations!
"""""""""""""""""""""""""""""""""" Call of Duty: Elite Fight Night!
Spike TV's Video Game Awards!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

New Research Shows Video Games Stimulate Kids Imaginations

We all know that parents should pay attention to both the amount of time kids spend playing video games and the type of games they're playing, but contrary to some prevailing wisdom, a new study shows that kids who play video games may actually be more creative than those who don't.

The study of 491 12-year-olds was conducted by lead researcher Linda Jackson, a professor of psychology at Michigan State University, as part of the Children and Technology Project. It found that the more kids played video games, the more creative they were in tasks like writing stories and drawing pictures, as gauged by the figural version of the Torrance Test of Creativity. The test uses picture-based exercises to measure mental characteristics like originality, elaboration, and emotional

expressiveness.

The study found that in general, boys played video games more than girls, and, perhaps not surprisingly, that boys also tended to play sports and violence based games while girls tended to favor games featuring interaction with others. The Entertainment Software Association reports that about 72% of households in the United States play video or computer games.

The study also found that use of technology other than playing video games, such as using cell phones, browsing the internet, or using a computer for other tasks, did not have a noticeable effect on creativity. Jackson is hopeful that video game designers will be able to use the results of the study to design games which can "blur the distinction between education and entertainment."

Call of Duty: Elite Fight Night Gives Famous Rivals A Chance To Settle It Digitally

And in this corner... When the Call of Duty: Elite service rolls out in conjunction with Call of Duty: Modern Warfare 3 next Tuesday, there will be both a free service as well as a premium version. The free service will offer new levels of stat tracking and several more options to expand the reach of the game, but for those that opt in for the premium version, membership has its privileges.

One of those privileges is access to ’Friday Night Fights,’ a weekly video series produced by Ridely and Tony Scott s RSA Productions, which will be released exclusively to Elite premium members. Each Friday two new rival groups will face off via Call of Duty: Modern Warfare 3. Sometimes it will be celebrities, other times it will be well-known group rivalries. Both sides will receive coaching from professional gamers, and the episodes will feature a slew of famous personalities to join in the fun. The winning side will then donate the proceeds - up to $5,000 - to the Call of Duty Endowment, a charitable group dedicated to helping returning soldiers find employment.

The series will premiere next Friday, November 11 on Veteran s Day, and feature the classic rivalry of Army vs. Navy. The series will continue each week through the rest of the year until the first season is complete.

Some of the famous groups and celebrities involved are:

* Celebrities:

o Music: Good Charlotte (Benji & Joel Madden), The Game, Cali Swag District

o Sports: Dwight Howard (Orlando Magic), John Wall (Washington Wizards)

o Actors: Michelle Rodriguez

o Personalities: Jack Osbourne

* Real world rivals:

o Army vs. Navy

o Police vs. Fireman

o New York city fans vs. Boston fans

The show will be hosted by model-turned-WWE Diva and current George Clooney squeeze, Stacy Keibler. The series will be part of the first batch of entertainment videos released as part of the Call of Duty: Elite, Elite TV, which will air several programs exclusively for subscribers. Will Arnett and Jason Bateman have also signed on to create original content, and more program announcements will be coming soon.

Call of Duty: Elite will be released on November 8. A year s worth of the premium service will be included as part of the Call of Duty: Modern Warfare 3 Hardened Edition, or it can be purchased separately for $49.99 per year.

Spike TV Hosts Video Game Awards Show

Emmy-winning producer Mark Burnett is taking on another awards show, this time Spike TV’s Video Game Awards next month.

The "Survivor" and "Celebrity Apprentice" producer says he’s very comfortable around video games, given that he’s regularly trounced at them by his three teenagers. They particularly enjoy "Black Ops" and "FIFA," he said.

"It’s an enormous industry. It’s going to get bigger and bigger and bigger," he told TheWrap. "It’s such a growing, dynamic industry, and it seemed a great way for me to absorb more and go beyond just passively enjoying video games, and get into it more, as well as bring my skill set to make it an epic awards show."

Burnett’s previous awards shows have included MTV’s VMAs and the Emmys.

"Mark’s bold producing style is a perfect fit for gamers, and his tremendous vision and unparalleled energy will take the show to a new level," said Casey Patterson, executive producer of the VGAs and executive vice president of event production for Viacom Media Networks Entertainment Group.

Besides handing out awards, the VGAs feature exclusive world premieres and teasers for some of the most-anticipated games. Guests include Hideo Kojima, who will premiere "Metal Gear Solid: Rising."

BioWare, creators of most anticipated game nominee "Mass Effect 3," will announce a new project and studio.

The VGAs telecast will premiere live, in high-definition, on Saturday, December 10 at 8 ET/5 PT.

=~=~=~=

A-ONE’s Headline News

The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Britain Warns Against State-Sponsored Cyberattacks

British Foreign Secretary William Hague warned foreign governments against state-sponsored cyberattacks Wednesday, hinting at a more confrontational approach if they don’t stop.

Hague, who was speaking at the close of a two-day conference on cybersecurity, was careful not to identify any countries by name, even when asked repeatedly about China.

He told reporters in London that Britain had not hosted a "judgmental conference" where participants sat around pointing fingers.

"It hasn’t been our approach in this conference to identify other countries and try to name and shame them," he said, before adding: "That may happen on other occasions."

In recent months a string of British officials have warned of the threat to the nation’s electronic infrastructure from foreign hackers, with much of the suspicion falling on Russia and China.

Earlier this week former security minister Pauline Neville-Jones, who now serves as the prime minister’s representative to business on cybersecurity, said Beijing and Moscow were "certainly" involved in that sort of activity.

In earlier comments on online censorship, Hague was more direct.

Asked about a Russo-Chinese proposal for an Internet "code of conduct," Hague said those countries’ attitudes toward free speech didn’t match his own.

He predicted that governments who attempted to resist "the tide that is flowing toward greater transparency and accountability" would fail.

Hague said he wouldn’t seek to square Chinese or Russian Internet policies with Britain’s, explaining that it was up to others to "square themselves" with free expression and an open Web.

US Report Blasts China, Russia for Cybercrime

U.S. intelligence officials accused China and Russia on Thursday of systematically stealing American high-tech data for their own national economic gain.

It was the most forceful and detailed public airing of U.S. allegations after years of private complaints. U.S. officials and cybersecurity experts said the U.S. must openly confront China and Russia in a broad diplomatic push to combat cyberattacks that are on the rise and represent a "persistent threat to U.S. economic security."

But experts said solving the problem won’t be easy.

In a report released Thursday, U.S. intelligence agencies said "the governments of China and Russia will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace."

Speaking at a forum at the National Press Club, Robert Bryant, the national counterintelligence executive, said the U.S. is finally making the charges public because China and Russia are stealing sensitive U.S. technology data.

"If we build their economies on our information, that’s not right," he said. "We want to basically point out what the issue is. We want to be worried and we want to be careful, but we also want there to be an awareness and, frankly, drive that toward solutions where we work together to bring this under control."

The report is part of an increased effort by U.S. officials to highlight the risks of cyberattacks in a growing high-tech society. People, businesses and governments are storing an increasing amount of valuable and sensitive information online or accessing data through mobile devices that may not be as secure as some computers.

The Obama administration has urged individuals and the corporate world to better protect their data. Thursday’s report is a clarion call, cybersecurity experts said.

"We should have done this years ago," said James Lewis, cybersecurity expert and senior fellow at the Center for Strategic and International Studies. "We’ve pretended it hasn’t been happening, but that’s not the case. I hope this is the first in a series of documents that lays out the huge problem the U.S. is facing."

The U.S. points fingers at Russian and Chinese intelligence services and corporations based in those countries or tied to the governments.

The intelligence report, however, did not say how many of the cyberattacks are government-sponsored and would not name other countries that pose similar but lesser threats. It suggested that U.S. allies may be using their access to American institutions to acquire economic and technology information.

China had no immediate response to the report, which was issued after normal business hours Thursday in Beijing.

China has consistently denied engaging in cyberspying and, at a regularly scheduled news briefing Wednesday, Foreign Ministry spokesman Hong Lei reiterated Beijing’s insistence that it also has been attacked.

"China is a major victim of hacking," Hong said. "China is ready to build, together with other countries, a peaceful, secure and open cyberspace order."

He added, "As for the remarks from certain quarters, I would point out that hacking attacks have no boundaries and are anonymous. Speculating on the origin of the attacks without investigation is neither professional nor responsible."

China has been linked to a number of high-profile breaches.

Google Inc., operator of the Internet's most popular search engine, disclosed two sophisticated attacks against its systems that it believes were launched from China. The disclosures touched a nerve for technologists, government officials and human rights advocates alike because of the unique roles Google and the Chinese government have in shaping what is seen - and not seen - on the Internet by citizens of the world's most populous country.

In one attack, some of Google's intellectual property was stolen in a computer attack that also targeted at least 20 other large companies. And earlier this year Mountain View, Calif.-based Google said it believes hackers in China broke into the Gmail accounts of several hundred people, including senior U.S. government officials, military personnel and political activists.

The report also noted other incidents linked to China:

* Last year computer security firm Mandiant reported that data was stolen from a Fortune 500 manufacturing company during business negotiations when the company was trying to buy a Chinese company.

* Earlier this year, McAfee traced an intrusion to an Internet protocol address in China and said intruders took data from global oil, energy and petrochemical companies.

While officials could not pin down an exact economic cost to the U.S. government and businesses, they said the losses are extremely significant.

"(China's) continued theft of sensitive economic information is a threat to our national security, hurts American businesses and workers, and causes incalculable harm to global economy," said the chairman of the House Intelligence Committee, Rep. Mike Rogers, R-Mich. "This once again underscores the need for America's allies across Asia and Europe to join forces to pressure Beijing to end this illegal behavior."

The escalating rhetoric carries its own political risks, particularly as the U.S. has tried to improve relations with China and Russia. China is a key lender and trading partner, and the U.S. has relied on Beijing to put pressure on its longtime ally North Korea to negotiate over its nuclear program.

Russia, meanwhile, is a key vote in the U.N. Security Council, particularly on issues involving Iran sanctions and nuclear arms reduction.

Both were Cold War enemies whose motives and government workings are often purposely opaque to American partners or competitors.

"We have to start being more confrontational," said Lewis, adding that the U.S. needs to have a more muscular trade policy and make sure that World Trade Organization rules are observed.

The report said foreign intelligence services have used independent hackers as proxies, thereby giving the agencies "plausible deniability."

And it also accused the Chinese of being "the world's most active and persistent perpetrators of economic espionage."

Attacks from Russia are a "distant second" to those from China, according

to the report. But it said Moscow’s intelligence services are "conducting a range of activities to collect economic information and technology from U.S. targets."

The report said some of the most desired data includes communications and military technologies, clean energy, health care, pharmaceuticals and information about scarce natural resources. Of particular note, the report said, is interest in unmanned aircraft and other aerospace technology.

U.S. officials have called for greater communication about cyberthreats among the government, intelligence agencies and the private sector. The Pentagon has begun a pilot program that is working with a group of defense contractors to help detect and block cyberattacks.

The report, issued by the national intelligence director’s office of the counterintelligence executive, comes out every two years and includes information from 14 spy agencies, academics and other experts.

"We have to do a lot to scare those other guys into thinking ’don’t do it or bad things will happen to you’ but after we do that, we have to solve it here, at home," said Alan Paller, director of research at SANS Institute, a computer-security organization.

"We need to say, ’if you allow your citizens to attack computers in our country, causing massive damage, we have the right to cause massive damage in your country.’"

China Scorns U.S. Cyber Espionage Charges

China on Friday dismissed a U.S. report on online spying as "irresponsible," rejecting the charge that China uses cyber espionage to steal lucrative U.S. trade and technology secrets.

The U.S. intelligence report said on Thursday China and Russia are using cyber espionage to steal U.S. trade and technology secrets to bolster their own economic development, which poses a threat to U.S. prosperity and security.

So much sensitive information sits on computer networks that foreign intruders can net massive amounts of valuable data with scant risk of detection, said the report to Congress.

Foreign intelligence services, corporations and individuals stepped up their efforts to steal information about U.S. technology that cost many millions of dollars to develop, according to the report by the Office of the National Counterintelligence Executive, a U.S. government agency.

But the Chinese Foreign Ministry spokesman Hong Lei rejected the report, and repeated Beijing’s long-standing position that it wants to help.

"Online attacks are notable for spanning national borders and being anonymous. Identifying the attackers without carrying out a comprehensive investigation and making inferences about the attackers is both unprofessional and irresponsible," Hong told a daily news briefing in answer to a question about the report.

"I hope the international community can abandon prejudice and work hard

with China to maintain online security," he added.

The U.S. report acknowledged the difficulty of determining who exactly is behind a cyber attack. U.S. companies have reported intrusions into their computer networks that originated in China, but U.S. intelligence agencies cannot confirm who specifically is behind them.

Intelligence officials say it is part of the national policy of China and Russia to try to acquire sensitive technology for their own economic development, while the United States does not do economic espionage as part of its national policy.

The State Department in June said it had asked Beijing to investigate Google’s allegation of a major hacking attack that the Internet giant said originated in China.

UK Says Governments’ Internet Power Grab Will Fail

Attempts by China, Russia and others to gain more control over the Internet are doomed to failure, Britain said on Wednesday, after hosting a major conference on cyberspace that it said sent a clear signal to authoritarian governments.

Speaking after the London conference attended by 60 nations, British Foreign Secretary William Hague said threats of cyberterrorism and cybercrime were real, but should not be used as a pretext for online repression.

"The conference agreed that efforts to improve cyber security must not be at the expense of human rights," he said, summing up the conference’s conclusions.

"My message to governments is that in the long term efforts to resist the freer flow of information, the tide that is flowing toward greater transparency and accountability, will fail."

The conference was designed to give fresh impetus to debates taking place in multiple forums about the future of cyberspace, including the growing threat of cybercrime, and the Internet’s potential for boosting economic growth.

China, Russia and some other fast-growing economies have been calling in recent months for a bigger say in how the Internet is run. It has until now been loosely governed by a collection of mainly Western-dominated bodies.

"I suspect London marks the emergence of two clear camps that have been coalescing this year," said one Western delegate, speaking on condition of anonymity.

"The Western agenda is now robustly declared and challenging for China. Will Russia and China decide to play or not?"

The conference was dominated by the United States and Europe, with U.S. Vice President Joseph Biden, European Commissioner Neelie Kroes and Facebook policy director Richard Allan among the top speakers.

Russia took part in the conference and stood by its call for a new international treaty or code of conduct for cyberspace to be established by governments.

China sent a small delegation but did not participate actively in the open sessions. It was barely mentioned by name during the conference despite the fact that more state-sponsored cyber attacks are believed to originate in China than in any other country.

Europe is hoping China will help bail out the euro zone, which sank deeper into crisis this week with Greece's call for a referendum on a financial rescue plan.

"I don't think you can simultaneously hold a conference of this kind, drawing governments into this discussion, and as people are coming to the door, point your finger at them all and say: 'You are guilty men,' so we are going about this in a diplomatic way," Hague said.

In his closing message, he said: "State-sponsored attacks are not in the interests of any country, long term... those governments that perpetrate them need to bring them under control." He did not name names.

Some private-sector delegates like Wikipedia founder Jimmy Wales were less reticent.

"People do realize that there are some legitimate problems and that those problems need solutions," he told Reuters in an interview. "The difficulty comes when you've got countries like China who maybe view freedom of speech as the problem that needs to be solved."

Canadian academic Rafal Rohozinski, an expert on cyber warfare and chief executive of the SecDev Group, said the West was under pressure to regain control of the agenda on Internet governance in the face of a growing bloc of developing nations that want more influence.

"The G8, the Euro-Atlantic alliance if you like, needs to come up with an effective counter-narrative," he told Reuters.

This week's event will be followed by conferences in Budapest in 2012 and Seoul in 2013.

CIA Tracks Revolt by Tweet, Facebook

In an anonymous industrial park, CIA analysts who jokingly call themselves the "ninja librarians" are mining the mass of information people publish about themselves overseas, tracking everything from common public opinion to revolutions.

The group's effort gives the White House a daily snapshot of the world built from tweets, newspaper articles and Facebook updates.

The agency's Open Source Center sometimes looks at 5 million tweets a day. The analysts are also checking out TV news channels, local radio stations, Internet chat rooms - anything overseas that people can access and contribute to openly.

The Associated Press got an apparently unprecedented view of the center's

operations, including a tour of the main facility. The AP agreed not to reveal its exact location and to withhold the identities of some who work there because much of the center’s work is secret.

From Arabic to Mandarin, from an angry tweet to a thoughtful blog, the analysts gather the information, often in a native tongue. They cross-reference it with a local newspaper or a clandestinely intercepted phone conversation. From there, they build a picture sought by the highest levels at the White House. There might be a real-time peek, for example, at the mood of a region after the Navy SEAL raid that killed Osama bin Laden, or perhaps a prediction of which Mideast nation seems ripe for revolt.

Yes, they saw the uprising in Egypt coming; they just didn’t know exactly when revolution might hit, says the center’s director, Doug Naquin.

The center already had "predicted that social media in places like Egypt could be a game-changer and a threat to the regime," he said in an interview.

The CIA facility was set up in response to a recommendation by the 9/11 Commission, its first priority to focus on counterterrorism and counterproliferation. Its predecessor organization had its staff heavily cut in the 1990s - something the CIA’s management has vowed to keep from happening again, with new budget reductions looming across the national security spectrum.

The center’s several hundred analysts - the actual number is classified - track a broad range of subjects, including Chinese Internet access and the mood on the street in Pakistan.

While most analysts are based in Virginia, they also are scattered throughout U.S. embassies worldwide to get a step closer to their subjects.

The center’s analysis ends up in President Barack Obama’s daily intelligence briefing in one form or another almost every day. The material is often used to answer questions Obama poses to his inner circle of intelligence advisers when they give him the morning rundown of threats and trouble spots.

"The OSC’s focus is overseas, collecting against foreign intelligence issues," said CIA spokeswoman Jennifer Youngblood. "Looking at social media outlets overseas is just a small part of what this skilled organization does," she said. "There is no effort to collect on Americans."

The most successful open source analysts, Naquin said, are something like the heroine of the crime novel "The Girl With the Dragon Tattoo," a quirky, irreverent computer hacker who "knows how to find stuff other people don’t know exists."

An analyst with a master’s degree in library science and multiple languages, especially one who grew up speaking another language, makes "a powerful open source officer," Naquin said.

The center had started focusing on social media after watching the Twitter-sphere rock the Iranian regime during the Green Revolution of 2009, when thousands protested the results of the elections that kept Iranian President Mahmoud Ahmadinejad in power. "Farsi was the third largest

presence in social media blogs at the time on the Web," Naquin said.

After bin Laden was killed in Pakistan in May, the CIA followed Twitter to give the White House a snapshot of world public opinion.

Since tweets can't necessarily be pegged to a geographic location, the analysts broke down reaction by language. The result: The majority of Urdu tweets, the language of Pakistan, and Chinese tweets, were negative. China is a close ally of Pakistan's. Officials in Pakistan protested the raid as an affront to their nation's sovereignty, a sore point that continues to complicate U.S.-Pakistani relations.

When President Obama gave his speech addressing Mideast issues a few weeks after the raid, the tweet response over the next 24 hours came in negative from Turkey, Egypt, Yemen, Algeria, the Persian Gulf and Israel, too. Tweets from speakers of Arabic and Turkic contended that Obama favored Israel, while Hebrew tweets denounced the speech as pro-Arab.

In the following days, major news media came to the same conclusion, as did analysis by the covert side of U.S. intelligence based on intercepts and human intelligence gathered in the region.

The center is also in the process of comparing its social media results with the track record of polling organizations, trying to see which produces more accurate results, Naquin said.

"We do what we can to caveat that we may be getting an overrepresentation of the urban elite," said Naquin, acknowledging that only a small slice of the population in many areas being monitored has access to computers and Internet. But he points out that access to social media sites via cellphones is growing in such areas as Africa, meaning a "wider portion of the population than you might expect is sounding off and holding forth than it might appear if you count the Internet hookups in a given country."

Sites such as Facebook and Twitter have become a key resource for following a fast-moving crisis such as the riots that raged across Bangkok in April and May of last year, the center's deputy director said. The AP agreed not to identify him because he sometimes still works undercover in foreign countries.

As director, Naquin is identified publicly by the agency although the location of the center is kept secret to deter attacks, whether physical or electronic.

Naquin says the next generation of social media will probably be closed-loop, subscriber-only cellphone networks, like the ones the Taliban uses to send messages among hundreds of followers at a time in Afghanistan and Pakistan. Those networks can be penetrated only by technical eavesdropping by branches of U.S. intelligence, such as the National Security Agency - but Naquin predicts his covert colleagues will find a way to adapt, as the enemy does.

Anonymous Exposes Visitors to Child Porn Sites

The online "hacktivist" group Anonymous claimed on Wednesday to have published the Internet Protocol addresses of nearly 200 visitors to child

pornography forums.

In a statement posted to pastebin.com, Anonymous said it was exposing the IP addresses as part of a campaign dubbed "Operation Darknet."

An IP address is the unique number used by every device that connects to the Internet.

Most of the IP addresses of visitors to child porn sites exposed by Anonymous were in the United States but some were located in Europe, Latin America and elsewhere.

Anonymous said it captured the IP addresses of visitors to child porn forums by tricking users into downloading a fake update to Tor software, which can be used to obscure an Internet user's identity.

The purported Tor update actually routed traffic to a forensics server controlled by Anonymous that logged incoming IP addresses and destination.

During a 24-hour period last week, Anonymous said it captured the unique IP addresses of 190 visitors to child porn forums.

Anonymous has been involved in scores of hacking exploits including the recent defacing of a website of Syria's Ministry of Defense to protest a bloody crackdown on anti-government protestors.

Last year, the shadowy group launched retaliatory attacks on companies perceived to be enemies of the anti-secrecy website WikiLeaks.

Who's Winning the Facebook-Google Tech War

When Google launched its Facebook doppleganger, Google+, it became clear that the two were in an war to win the Internet. Google ruled the Web for awhile, but little underdog Facebook crept up and all of a sudden its social networking site had 800 million very active users. Now the two are in a bona-fide war, explains Fortune's Miguel Helft. "In the long history of tech rivalries, rarely has there been a battle as competitive as the raging war between the web's wonder twins," he writes. One could argue that one is better than the other, preferring Google+'s circles to Facebook's Timeline, but this is really a numbers game.

Google: Google has the largest share of the ad market than any single tech company, nabbing 41 percent of the $31 billion U.S. online ad market. And it's basically got the ad search market cornered.

Facebook: Facebook may not have all that ad power, but its ad-revenue is growing at a super-fast 81 percent this year.

Winner: Tie Hands down, Google brings in more money. But the trends aren't working in its favor. "Advertisers are putting more of their limited dollars into Facebook, with its 800 million users, many of whom spend more time on Facebook than on any other site," writes Helft. Google's display ad dollars will grow a measly 34 percent, peanuts compared to Facebook's expected growth. There is one big however, though, for Facebook. The company hasn't quite been able to monetize all the ad attention its getting very well. It can attract big names, like Ford, but these companies aren't spending too much to advertise on Facebook, as The Wall

Street Journal’s Emily Steel and Geoffrey Fowler noted. "Everybody wants to be liked," they write. "The question for Facebook Inc. is how much advertisers are willing to pay for the opportunity."

Google: Google rakes in almost nine times as much as Facebook, and is expected to grow to $38 billion this year.

Facebook The social network is expected to more than double its revenue this year to $4.3 billion.

Winner: Google Facebook’s growth rate trumps Google’s 30 percent growth. But having that lump of cash means Google can buy popularity and growth. Just this year, Google spent $12.5 billion (Facebook times 3) to acquire Motorola. "Page can afford these big swings (and others) in the years ahead, given the way his advertising business just keeps growing," Fast Company’s Farhad Manjoo pointed out.

Google In trying to keep its most talented people around, Google shot itself in the foot. After losing talent, Google offered top engineers big $10 million in equity-and-cash deals to stay, an executive told Helft. Smarty pants Google employees leveraged that, seeking offers from Facebook to get raises. Google changed its strategy, offering a company wide 10 percent raise. In short: Google’s spent a lot of money to keep people around.

Facebook Facebook has successfully stolen away Google’s best. "Four of Facebook’s 11 top executives hail from Google, including COO Sheryl Sandberg and David Fischer, the advertising and operations chief," explains Helft.

Winner: Facebook Google spent big money to keep its gold and in doing so ruined its cred. "It created an un-Googley environment," senior manager who left Google recently told Heflt. And Facebook still won over those coveted Googlers.

It’s a close race. Facebook’s all about growth this and growth that. But then again, Google does have all that money with which to squash Facebook.

Copyright and Wrong

A piece of legislation backed by the MPAA was introduced in the House of Representatives this week and threatens to upend the way we use the Internet.

The E-Parasites Act, a contrived acronym for Enforcing and Protecting American Rights Against Sites Intent on Theft and Exploitation, seeks to give the attorney general broad power to create a blacklist of websites that ’induce’ copyright infringement. Service providers would then be legally compelled to block these websites.

Let s say you re using an online digital locker service like Dropbox to store your Microsoft Word files. Someone else on the site, however, is using it to house illegally downloaded MP3s. The record label finds out, approaches a judge and says, "Dropbox is inducing its users to commit copyright infringement. We request you block it, or we ll go to MasterCard - which handles Dropbox s money matters - or the site s advertisers and

legally demand that they stop facilitating the site s inducement of copyright infringement."

The law can either shutter a website until it removes copyright-violating material or financially ruin it. In either scenario, your Word files are gone.

Should the E-Parasites bill become law, virtually every company on the Internet will be expected to constantly patrol their users for copyright infringement. It also effectively neutralizes the ’safe harbor’ part of the Digital Millennium Copyright Act, or DMCA, that protects companies from being prosecuted after copyright material has been uploaded to their websites.

It would be pretty difficult for Twitter and YouTube to exist if they had to constantly monitor and scan every single tweet for verboten content. Sure, illegitimate websites would be hampered, but experts feel it would place unprecedented economic burdens on legitimate ones.

"This bill is a disaster," said Electronic Frontier Foundation staff attorney Corynne McSherry. "It s a jobs-killer that would hurt legitimate businesses. In this type of economic environment, we should be trying to create jobs, not destroy them."

The Motion Picture Association of America disagrees with that assessment, arguing that ’rogue websites’ cost millions of jobs and dollars worth of damage in the process.

Sound like geek-speak to you? Think again. Many of today s most popular websites and services that we use every day depend on those DMCA safe harbors. Put it this way: The only reason YouTube, Facebook and a host of others are able to exist is because these safe harbors protect them from destructive litigation, or worse. If E-Parasites goes into effect, rights holders can go to companies like MasterCard and PayPal, tell them that YouTube is engaging in copyright infringement, then tell them to cut off funding. And if that happens, say bye-bye to YouTube.

"No American wants to be told what website they re allowed to go to," said Holmes Wilson, co-founder of the Fight for the Future digital advocacy group. "If this passes, you could go to Dropbox in the morning and find a message from the government saying it was blocked."

In effect, the law would create a separate, ’America-approved’ Internet, just like the kind found in China with its Great Firewall. The move would "send signals to oppressive regimes around the world that censoring the Internet is OK so long as it s done in the name of intellectual property," said McSherry.

Then there s the technical side to consider. To block ’rogue’ websites, the proposed law interferes with the technology that translates easy-to-remember website names into their actual numbered addresses. (Do you really trust Washington bureaucrats with one of the Internet s most vital technologies?) But if you happened to know the numerical IP address of a website - a quick Google search will reveal it - you d be able to bypass the roadblock and visit the site.

So in the unlikely event that thedaily.com gets blocked, you d be able to reach it by typing 50.16.191.138 into your address bar.

Said McSherry: "Interfering with the Internet is not how you protect it."

The Right To Dual-Boot: Linux Groups Plead Case Prior to Windows 8 Launch

Red Hat, Canonical and the Linux Foundation have laid out a set of recommendations for hardware vendors in hopes of preserving the ability to install Linux on Windows 8 machines. Windows 8 machines should ship in a setup mode giving users more control right off the bat, the groups argue.

As we reported last month, Windows 8 computers that ship with UEFI secure booting enabled could make the task of replacing Windows with Linux or dual-booting the two operating systems more difficult. In order to get a ’Designed for Windows 8’ logo, PCs must ship with secure boot enabled, preventing the booting of operating systems that aren t signed by a trusted Certificate Authority.

Hardware vendors can give users the option of disabling the secure boot feature - but they could also decline to do so, making it impossible to run a non-Windows operating system. In practice, it seems unlikely that dual-boot scenarios will be prevented entirely, but Linux vendors and the Linux Foundation are worried about how UEFI secure booting will be implemented.

In a paper titled "UEFI Secure Boot Impact on Linux," Red Hat and Canonical warn that "Microsoft s recommended implementation of secure boot removes control of the system from the hardware owner, and may prevent open source operating systems from functioning." Although Windows 8 isn t expected to hit the market until later in 2012, the paper notes that hardware vendors could start shipping UEFI-enabled systems in Q1 2012 in preparation for Windows 8.

Red Hat and Canonical agree that UEFI secure boot brings security advantages in malware prevention by protecting against rootkits and in giving IT departments ability to dictate that only authorized OSes can be booted. But given the potential impact on the freedom to install Linux and other alternative operating systems, the open source vendors offer a few recommendations.

These include that ’OEMs allow secure boot to be easily disabled and enabled through a firmware configuration interface,’ that hardware vendors ’provide a standardized mechanism for configuring keys in system firmware’; and that ’hardware ship in setup mode,’ giving the end user more control right up front.

How much control do users want?

This last recommendation could be problematic for hardware vendors attempting to give a clean out-of-the-box experience to users, the vast majority of whom simply want to use Windows and get the system up and running quickly.

Red Hat and Canonical argue that "If the process required to disable secure boot is difficult for non-technical users, then we risk restricting use of unsigned software to a small portion of the market." One could also argue that Linux installations are already restricted to a small portion of the market, which tends to be technically savvy enough to work around the restrictions expected in UEFI-enabled systems. However, Red Hat and Canonical may be worried that future attempts to bring Linux desktops to

the mainstream will be impeded.

In a separate paper titled "Making UEFI Secure Boot Work With Open Platforms," the Linux Foundation makes a recommendation similar to the one offered by Red Hat and Canonical, saying ’all platforms that enable UEFI secure boot should ship in setup mode where the owner has control over which platform key (PK) is installed. It should also be possible for the owner to return a system to setup mode in the future, if needed.’

The Linux Foundation further supports the establishment of an independent certificate authority to issue keys to third-party hardware and software vendors, presumably allowing Linux-based operating systems to be installed and still gain the security benefits of UEFI secure boot. (The Free Software Foundation has also weighed in with a petition directed at hardware vendors.)

Microsoft, for its part, noted in a blog post last month that it does not ’mandate or control the settings on PC firmware that control or enable secured boot from any operating system other than Windows,’ but says UEFI secure boot addresses a pre-operating system environment that is vulnerable to attack.

"At the end of the day, the customer is in control of their PC," Microsoft says. Without mentioning Linux by name, Microsoft said "For the enthusiast who wants to run older operating systems, the option is there to allow you to make that decision."

Indeed, as we noted last month, the Windows 8 developer system built by Samsung and distributed at Microsoft s BUILD conference contains the option to disable secure boot. Since few computers ship with Linux pre-installed, Linux groups hope that same option will be available on all Windows 8 systems, and that it will be easily accessible even for users who aren t Linux experts.

Stupid Hacker Tricks: Exploits Gone Bad

If the Internet is the new Wild West, then hackers are the wanted outlaws of our time. And like the gun-slinging bad boys before them, all it takes is one wrong move to land them in jail.

Whether they are out to steal money or merely wreak havoc, the consequences of an exploit gone bad can be harsh. And these days, the margin for error can be measured in bits. After all, thanks to the Internet’s international nature, cyber outlaws have an awful lot of sheriffs sniffing out their online footsteps.

[For more real-world tales of brain fail, see "Stupid user tricks 5: IT’s weakest link." * Find out which of our eight classic IT personality types best suit your temperament by taking the InfoWorld IT personality type quiz. * Get a $50 American Express gift cheque if we publish your tech tale from the trenches. Send it to offtherecord@infoworld.com.]

Sometimes, though, the sheriffs don’t have to work too hard. Clever as they often are, hackers can turn boneheaded pretty quickly and slip up in silly ways, leaving authorities a virtual road map pointing right to their doorsteps.

Just ask the suspects in these five cases, all of whom have officially earned a spot in InfoWorld’s Stupid Hacker Tricks Hall of Shame.

Stupid hacker trick No. 1: Hack, tweet, repeat - until arrested
The suspect: Scott Arciszewski

The crime: Hacking an FBI-sponsored website

Dossier: Arciszewski is accused of hacking into the website of InfraGard, an FBI-run program focused on cyber crime prevention. Yes, you read that correctly: cyber crime prevention. In other words, if there were an encyclopedia entry for "places you don’t want to mess with," InfraGard would top the list.

Common sense be damned, though, someone decided InfraGard needed to be infiltrated. Apparently the company’s ties with the government rubbed some folks the wrong way; this past June, the hacking collective known as LulzSec took credit for taking down one of the organization’s sites, citing recent computer crime legislation as the cause of its ire.

The incident connected to Arciszewski came just one month later, in July 2011. The FBI alleges that Arciszewski, a 21-year-old computer engineering major at the University of Central Florida, broke into InfraGard’s Tampa Bay chapter website. He’s accused of uploading a few files - animated kitty GIFs, one can only hope - and then posting a link on Twitter showing others how he skirted the website’s security.

The tweet reportedly contained just eight words - "Infraguard [sic] Tampa has one hell of an exploit" - along with a shortened link. That turned out to be more than enough to send the bloodhounds on Arciszewski’s path.

The bust: FBI agents, none too pleased with their public flogging, set out to find the guy who tore a hole in their virtual fence. It didn’t take too much work, from the sounds of it: According to reports, Arciszewski retweeted his boast to the attention of the FBI’s official press office account. D’oh!

"Word of mouth leads to a lot of arrests," says Clifford Neuman, director of the USC Center for Computer Systems Security. "Hackers often brag to others on message boards and social [media] services, so detectives look for indications like online postings and then start tracing forward from that activity."

In Arciszewski’s case, the feds tracked down the IP address used in the attack and connected it to that troublesome tweet. According to Ryan J. Reilly at TPM Idea Lab, the FBI went from Arciszewski’s Twitter account to his personal website. Before long, they found his real name, matched up some photos, and showed up at his UCF dorm room with a warrant for his arrest.

On the plus side, that may have been the most action Arciszewski’s dorm saw all semester.

Stupid hacker trick No. 2: RisquØ Miley Cyrus pics arouse suspicion
The suspect: Josh Holly

The crime: Hacking celebrities’ Internet accounts as part of a spam and credit card-stealing caper

Dossier: It’s no party in the U.S.A. these days for Josh Holly, the 21-year-old accused of hacking Miley Cyrus’s Gmail account and posting provocative pics of her online. Holly is currently facing criminal charges - though, in a surprising twist, not for the semi-indecent exposure of the then-15-year-old star.

Holly’s trouble actually revolves around a series of spam-based credit card thefts. In August, he pleaded guilty to felony charges stemming from the possession of about 200 compromised credit card numbers. According to the FBI, Holly hacked into numerous celebrities’ MySpace accounts, then used their accounts to spam the masses, reaching legions of responsive followers and bringing in more than $100,000 in shadily obtained revenue.

So where does the lovely Ms. Cyrus factor into the equation? Holly famously bragged about breaking into Miley’s email and stealing her risquØ photos (which, of course, were plastered all over the Web in no time). Holly told Wired the whole thing started when he broke into a MySpace admin panel and found a plain-text list of passwords. He tried Miley’s MySpace password on a Gmail account she was known to use, according to the interview - and sure enough, it worked.

The bust: Though Holly was never charged specifically for the Miley incident, that high-profile hack appears to have played an integral role in his arrest. The FBI followed his boastful bread crumbs and raided his Tennessee home. They seized his computer and found all the evidence they needed inside.

Holly seemed to spot his slip-ups pretty quickly - after the fact, at least. In an interview conducted with Wired shortly after his arrest, Holly is quoted as saying, "There’s no way I can get out of this. ... I was an idiot and I didn’t delete any of my [hard drive data]. I never thought they would raid me. They’re going to get full proof [sic] evidence of everything that I’ve said I’ve done."

Of course, the massive amounts of money moving through various accounts probably didn’t help, either. Where there’s money, after all, there’s almost always a trail.

"Whenever there is required collusion - the exchange of a hack or credit card number or anything like that - that creates a point of vulnerability where information can be exposed," USC’s Neuman explains.

Holly could face up to 10 years in prison and a $250,000 fine.

Stupid hacker trick No. 3: Boost score, get busted
The suspect: An unnamed 17-year-old from Manchester, U.K.

The crime: Launching a DDoS attack on the Call of Duty website and bringing the game to a screeching halt

Dossier: The British teen is accused of using a tool called Phenom Booter to perform a DDoS attack on the servers responsible for hosting the popular Call of Duty video game. According to U.K. media reports, the boy’s goal was to keep other players from signing in and killing his character - thereby allowing him to maintain a high score.

Ah, kids.

To his credit, the plot worked. It reportedly took the Call of Duty staff several hours to get the site back up and running. In the meantime,

countless users were unable to get online and play.

Our junior hacker didn’t stop with the single attack, though. Investigators say he spent time scouting out other would-be hackers and offering to sell them the secret to his score-boosting ruse.

The bust: Police tracked the teen to his home - where you can imagine Mum and Dad were none too pleased.

While hackers often use proxies and redirection services to mask their locations, it sounds like our amateur attacker didn’t do much to hide. Officers say they quickly figured out that the server responsible was hosted in the United Kingdom. From there, it didn’t take them long to make their way to the Manchester neighborhood where Boy Wizard lived.

"Hackers only need to make a mistake once for that to be the piece of evidence which ultimately identifies them," says Graham Cluley, senior tech consultant at Sophos.

Needless to say, this little prank didn’t have police laughing. "This type of crime can often be the precursor to further offending in more traditional areas of online crime," detectives told the Daily Mail.

"Spanky, spanky," the kid’s parents probably added.

Stupid hacker trick No. 4: Pummel PayPal, get payback
The suspects: Christopher Cooper, Joshua Covelli, Keith Downey, Mercedes Haefer, Donald Husband, Vincent Kershaw, Ethan Miles, James Murphy, Drew Phillips, Jeffrey Puglisi, Daniel Sullivan, Tracy Valenzuela, Christopher Vo, and one unnamed minor

The crime: Conducting a DDoS attack against PayPal

Dossier: When a handful of financial companies decided to stop handling payments for donations to WikiLeaks last December, the Internet temporarily went wild. Hackers from the group Anonymous cocked their guns and fired, promising to take down anyone "bowing down" to what they called "government pressure" to muzzle WikiLeaks’ efforts.

For PayPal, that meant a bunch of bogus Internet traffic. Hackers around the country conducted a DDoS attack against the site, allegedly using a tool called "Low Orbit Ion Cannon" to send massive amounts of data into PayPal. The goal, of course, was to overwhelm the company and cause its service to collapse.

The bust: A "Low Orbit Ion Cannon" sounds impressive - but apparently, the tool did a poor job of hiding its operators’ locations. PayPal was reportedly able to identify the IP addresses of different attackers in its server logs, allowing authorities to use that data to dig up the suspects.

"Even if hackers do redirect through other sites, it’s frequently still possible to track an attack back to them," USC’s Neuman notes. "You trace it back to one point, then you go through diplomatic channels to get the authorities in the outside country to find and collect the logs. It’s a months-long process, but it can be done."

In this case, that kind of international effort wasn’t even needed. FBI agents conducted raids on the suspects’ homes and made their arrests. And remember: For someone with something to hide, a raid can spell serious

trouble.

"When they arrest them, they've got warrants," Neuman says. "Even though the path back to them may have been somewhat obscured, they usually have information on their own machines that shows they had the source code or program related to the attack. A lot of individuals don't think it will ever get to that point and don't even try to prepare."

Each suspect is charged with conspiring to cause damage and intentionally causing damage to a protected computer - charges that, combined, carry penalties of up to 15 years in prison and $750,000 in fines. Some payback indeed.

Stupid hacker trick No. 5: Chat up your iPad account hack, end up in the clink. The suspects: Andrew Auernheimer and Daniel Spitler

The crime: Hacking into an AT&T database and exposing the email addresses of thousands of iPad owners

Dossier: Aurenheimer and Spitler discovered a public script on AT&T's website in which you could plug an ICCID number - a unique identifier associated with each iPad's SIM card - and get back the email address of the user who owns the device.

Armed with that knowledge, the two men, allegedly operating as "Goatse Security," are accused of creating their own script called the "iPad 3G Account Slurper." That script is said to have input random ID numbers in rapid-fire succession. Every time it came across a legitimate one, investigators say, it retrieved and logged the corresponding email address.

Harmless, right? Not quite: The script harvested more than 100,000 email addresses in all, including those of folks like New York Mayor Michael Bloomberg, former White House Chief of Staff Rahm Emanuel, and numerous other national leaders. And the guys from Goatse didn't keep the info quiet: The company is accused of offering the data to both News Corp. and Thomson Reuters. It was Gawker, however, that eventually bit and published a glimpse of the stolen tidbits, causing an embarrassing debacle for AT&T and Apple alike.

The bust: Once the data dump went public, the pressure was on to find the responsible parties. In this instance, once again, the old adage "loose lips sink ships" may describe what brought Goatse Security down.

In their complaint against Aurenheimer and Spitler, prosecutors cite numerous emails and chat logs in which the men appear to discuss the hack and their involvement. One note even mentions the possibility of "iPad focused spam" - something that certainly doesn't look good for anyone mulling over the men's intentions.

"In the cases of less-professional cyber criminals, they may find it irresistible to brag online about their activities, or leave nicknames in their attacks, which ultimately help authorities unmask them," Cluley points out.

Unmasked, perhaps - but hey, at least their email addresses weren't exposed.

How AOL Gets 3.5 Million People to Keep Paying for Dial-Up

The secret to AOL's 3.5 million dial-up subscribers: they're not paying for dial-up. Completely baffled the fact that not only do 3.5 million people still subscribe to AOL's dial-up service, but the company signed up 200,000 new subscribers just this year, we asked AOL spokeswoman Maureen Sullivan let us in on their magic. "We've been able to offer increased subscription offerings to our long term customers, who in some cases don't want or need dial-up access," she told The Atlantic Wire. "What other services can we provide to them, that they value?" AOL asked itself. So it keeps the money rolling in by offering other important services, like McAfee Security and Suzanne Sommers Sexy Forever, a weight loss program for women over 40.

The AOL subscriptions come in various flavors, ranging in prices from $9.99 per month for a bare-bones package to $25.90 per month for the highest level "AOL Total Advantage." It is not a great business. In the company's latest earnings release, revenues from subscriptions were down 22 percent. But it's still big money with $192 million in subscriptions reported for the quarter, 36 percent of the entire company's revenues. This is how they described the mini-boom in new subscriptions in their earnings release:

Subscription revenue declines reflect a 15 percent and 3 percent decline in domestic AOL-brand access subscribers and average revenue per subscriber, respectively. During the quarter, AOL began a price rationalization program and migrated certain individuals who did not previously receive access service (and therefore were not included as domestic AOL-brand access subscribers) to a higher priced plan with additional services that included access service. As a result, domestic AOL-brand access subscribers increased by approximately 200,000, leading to a lower year-over-year rate of decline than we have seen in recent quarters.

Some of those subscriptions, Sullivan told us, also apparently include people who live in areas without access to broadband. And another subset of people use it as a backup. But that really doesn't sound all too appealing. Reverting back to dial-up from Broadband sounds like death. Remember how long it took to download those Napster songs? Days! Considering how far Internet has come from its screechy, sloth-like roots, the continued existence of AOL's dial-up business and growing subscriber base astounded the Internet. But it turns out that these people aren't just paying for dial-up they're paying for other services. You can check out the full list of "deals" at what AOL calls its Lifestore. We guess AOL's just very good at scaring people into selling security systems?

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.